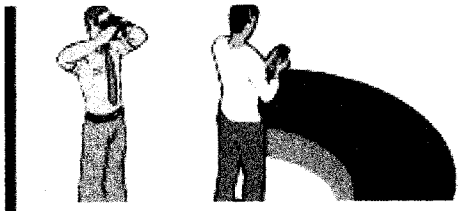
Cell Phone Tracking

The Wall Street Journal - WSJ Blogs

"What They Know – Mobile"
http://blogs.wsj.com/wtk-mobile/

Marketers are tracking smartphone users through "apps" - games and other software on their phones. Some apps collect information including location, unique serial-number-like identifiers for the phone, and personal details such as age and sex. Apps routinely send the information to marketing companies that use it to compile dossiers on phone users. As part of the What They Know investigative series into data privacy, the Journal analyzed the data collected and shared by 101 popular apps on iPhone and Android phones (including the Journal's own iPhone app). This interactive database shows the behavior of these apps, and describes what each app told users about the information it gathered.



Do you think apps should tell you when they collect and send information about the mobile device?

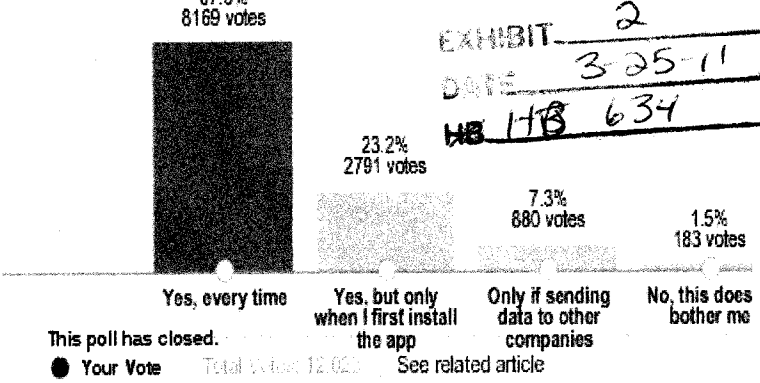


EXHIBIT 2
DATE 3-25-11
HB 1TB 634

THE WALL STREET JOURNAL.

iPhone | Android

Does not transmit data
Transmits data to app owner
Transmits data to third parties

App name	Username, Password	Contacts	Age, Gender	Location	Phone ID	Phone number
0.03 Seconds Pro					■	
Age My Face					■	
Angry Birds	■	■		■	■	
Angry Birds Lite	■			■	■	
Aurora Feint II: Lite	▥			■	■	
Barcode Scanner (BahnTech)					■	
Bejeweled 2	■					■
Best Alarm Clock Free				■	■	
Bible App (LifeChurch.tv)				■	■	
Bump						
CBS News				■	■	
0.03 Seconds					■	
Dictionary.com				■	■	
Doodle Jump	■				▥	

"The Tracking Ecosystem" - *The Wall Street Journal*

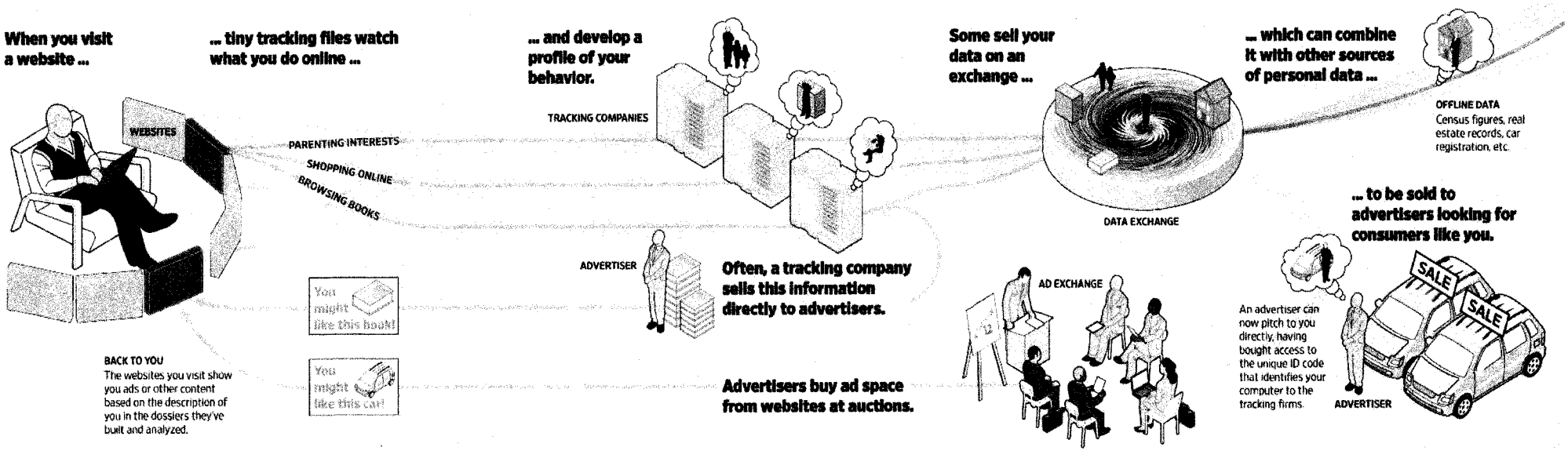


Image source:http://graphicsweb.wsj.com/documents/divSlider/ecosystems100730.html

---

A [Wall Street] Journal investigation finds that one of the fastest-growing businesses on the Internet is the business of spying on consumers.

Consumer tracking is the foundation of an online advertising economy that racked up $23 billion in ad spending last year. Tracking activity is exploding. Researchers at AT&T Labs and Worcester Polytechnic Institute last fall found tracking technology on 80% of 1,000 popular sites, up from 40% of those sites in 2005.

The Journal found tracking files that ***collect sensitive health and financial data****. On Encyclopaedia Britannica Inc.'s dictionary website Merriam-Webster.com, one tracking file from Healthline Networks Inc., an ad network, scans the page a user is viewing and targets ads related to what it sees there. So, for example, a person looking up depression-related words could see Healthline ads for depression treatments on that page—and on subsequent pages viewed on other sites.*

...Targeted ads can get personal. Last year, Julia Preston, a 32-year-old education-software designer in Austin, Texas, ***researched uterine disorders online****. Soon after, she started noticing fertility ads on sites she visited. She now knows she doesn't have a disorder, but* ***still gets the ads.*** *It's "unnerving," she says.*

Source: **"The Web's New Gold Mine: Your Secrets"** - The Wall Street Journal, 7/30/2010
http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html

Children Tracked on the Web

A Wall Street Journal investigation into online privacy has found that ***popular children's websites install more tracking technologies*** *on personal computers than do the top websites aimed at adults.*

The Journal examined 50 sites popular with U.S. teens and children to see what tracking tools they installed on a test computer. As a group, the sites placed 4,123 "cookies," "beacons" and other pieces of tracking technology. That is 30% more than were found in an analysis of the 50 most popular U.S. sites overall, which are generally aimed at adults.

*...**Selling the data is legal, but controversial**, especially when it involves young people. Two companies identified by the Journal as selling teen data initially denied doing so. Only when shown evidence that they were offering data for sale—in one case, it was labeled "teeny boppers"—did they confirm it.*

Source: "On the Web, Children Face Intensive Tracking" - The Wall Street Journal, 9/17/2010

http://online.wsj.com/article/SB10001424052748703904304575497903523187146.html

---

Price Discrimination and Loan Evaluation:

...New York-based Demdex Inc., for instance, helps websites build "behavioral data banks" that tap sources including ***online-browsing records, retail purchases*** *and a database predicting a person's* ***spot in a corporate hierarchy.***

"If we've identified a visitor as a midlife-crisis male," says Demdex CEO Randy Nicolau, a client, such as an auto retailer, can "give him a different experience than a young mother with a new family." The guy sees a red convertible, the mom a minivan.

The technology ***raises the prospect that different visitors to a website could see different prices as well.*** *Price discrimination is generally legal, so long as it's not based on race, gender or geography, which can be deemed "redlining."*

In financial services, fair-lending laws prohibit discrimination based on race, color, religion, national origin, gender, receipt of public assistance or marital status. The laws also require that borrowers have access to any data used to evaluate their creditworthiness.

But the law doesn't specifically bar using web-browsing history to make lending decisions. That means, in theory, ***a bank could deny a loan based on knowledge of the applicant's visits to, say, gambling sites.***

Source: "The Web's Cutting Edge, Anonymous in Name Only" - The Wall Street Journal, 8/4/2010
http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html

---

Matching Real Names to Web Browsing (and more)

*...**[P]ossessing real names** means RapLeaf can build **extraordinarily intimate databases** on people by tapping voter-registration files, shopping histories, social-networking activities and real estate records, among other things.*

*"Holy smokes," says Mrs. Twombly, 67 years old, after The Wall Street Journal decoded the information in RapLeaf's file on her. "**It is like a watchdog is watching me**, and it is not good."*

Source: "A Web Pioneer Profiles Users by Name," The Wall Street Journal, 10/25/2010
http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html

"And You Thought a Prescription Was Private"

The New York Times, 8/9/2009
http://www.nytimes.com/2009/08/09/business/09privacy.html

MORE than 10 years after she tried without success to have a baby, Marcy Campbell Krinsk is still receiving painful reminders in her mail. The ads and promotions started after she bought fertility drugs at a pharmacy in San Diego.

Marketers got hold of her name, and she found coupons and samples in her mail that shadowed the growth of an imaginary child — at first, for Pampers and baby formula, then for discounts on family photos, and all the way through the years to gifts suitable for an elementary school graduate.

"I had three different in vitro procedures," said Ms. Krinsk, now 55, a former telecommunications executive who lives with her husband in San Diego. "To just go to the mailbox and get that stuff, time after time after time, it was just awful."

Like many other people, Ms. Krinsk thought that her prescription information was private. But in fact, prescriptions, and all the information on them — including not only the name and dosage of the drug and the name and address of the doctor, but also the patient's address and Social Security number — are a commodity bought and sold in a murky marketplace, often without the patients' knowledge or permission.

That may change if some little-noted protections from the Obama administration are strictly enforced. The federal stimulus law enacted in February prohibits in most cases the sale of personal health information, with a few exceptions for research and public health measures like tracking flu epidemics. It also tightens rules for telling patients when hackers or health care workers have stolen their Social Security numbers or medical information, as happened to Britney Spears, Maria Shriver and Farrah Fawcett before she died in June.

"The new rules will plug some gaping holes in our federal health privacy laws," said Deven McGraw, a health privacy expert at the nonprofit Center for Democracy and Technology in Washington. "For the first time, pharmacy benefit managers that handle most prescriptions and banks and contractors that process millions of medical claims will be held accountable for complying with federal privacy and security rules."

The law won't shut down the medical data mining industry, but there will be more restrictions on using private information without patients' consent and penalties for civil violations will be increased. Government agencies are still writing new regulations called for in the law.

Ms. Krinsk was never able to find out who sold her information, but companies that have been accused in lawsuits of buying and selling personal medical data include drugstore chains like Walgreens and data-mining companies like IMS Health and Verispan. CVS Caremark, which handles prescriptions for corporate clients, has also been accused of violating patients' privacy.

These companies all say that names of patients are removed or encrypted before data is sold, typically to drug manufacturers.

But as Ms. Krinsk's case shows, there are leaks in the system.

Before the changes, privacy regulations mainly applied to hospitals and doctors. Enforcement was weak, and there were lots of loopholes.

Privacy experts cite research by Latanya Sweeney, director of the Data Privacy Lab at Carnegie Mellon University in Pittsburgh, which shows that a computer-savvy snooper can easily match names, addresses, Social Security numbers and so on to "re-identify" information that had supposedly been rendered anonymous.

"Our biggest concern is the complete lack of protection against re-identifying data that was supposed to be anonymous and secure," Ms. McGraw said.

TRACKING prescriptions has been a big business for decades. Data miners say their research is valuable because gathering and analyzing information from thousands of people helps identify trends and provides indications of potentially dangerous side effects of drugs.

"Data stripped of patient identity is an important alternative in health research and managing quality of care," said Randy Frankel, an IMS vice president. As for the ability to put the names back on anonymous data, he said IMS has "multiple encryptions and various ways of separating information to prevent a patient from being re-identified."

"De-identified health information is our core business," he said.

IMS Health reported operating revenue of $1.05 billion in the first half of 2009, down 10.6 percent from the period a year earlier. Mr. Frankel said he did not expect growing awareness of privacy issues to affect the business.

CVS Caremark says it is careful about patient data. "In very limited circumstances, we exchange aggregated, de-identified data with third parties to assist the health care community in understanding patient use of prescription medications with the goal of achieving better health outcomes," said Carolyn Castel, a company spokeswoman.

Selling data to drug manufacturers is still allowed, if patients' names are removed. But the stimulus law tightens one of the biggest loopholes in the old privacy rules. Pharmacy companies like Walgreens have been able to accept payments from drug makers to mail advice and reminders to customers to take their medications, without obtaining permission. **Under the new law, the subsidized marketing is still permitted but it can no longer promote drugs other than those the customer already buys.**

The ban on marketing is even more strict in California, where Walgreens is fighting off a class-action lawsuit filed on behalf of customers who received the subsidized mailings before the state outlawed them in 2004. Michael Polzin, a Walgreens spokesman, defended the mailings as a cost-cutting measure. "Patients who fail to properly take their medication cost the U.S. health care system $177 billion a year," when they fall sick and need treatment, he said.

The data mining industry, meanwhile, is challenging laws in New Hampshire, Maine and Vermont that ban collecting and selling prescription information to drug makers, which use it to decide which doctors to market to.

The companies in the case, IMS Health and Verispan, now part of the private company SDI Health, said the identities of patients were removed. "At no time does SDI ever receive any identifiable patient information nor any means to identify any patient from the data we handle. All data is de-identified prior to transmission to SDI," said Andrew Kress, chief executive of SDI.

Privacy advocates and a judge in the case argued that de-identified information could easily spin out of control. **"This information quickly finds its way into other databases, including those of insurance carriers and pharmacy benefits managers,"** Judge Bruce M. Selya wrote in a

federal appeals court decision upholding the New Hampshire law.

IN another big change, the stimulus law provides $19 billion to push doctors toward installing electronic records systems. It is a milestone on the road toward President Obama's goal of digitizing all medical records within five years. But digitization creates the potential for more abuses by hackers, as well as blackmail and insurance fraud.

"Privacy is under greater duress than ever before as medical records are switched from paper to electronic," said Pam Dixon, a consumer advocate and executive director of the World Privacy Forum near San Diego.

Administration officials say privacy guarantees are essential. "We can't afford to go forward with our plans unless we have assured the American public that the privacy of their information is assured," said Dr. David Blumenthal, the Health and Human Services Department's national coordinator for health information technology.

Companies like Google, Microsoft and WebMD see a lucrative business opportunity in assembling and holding personal health records. Patients and their doctors would be able to consult the records wherever and whenever needed. But the companies themselves recognize that they have work to do to persuade consumers and physicians that records will be safe and protected.

Although as many as one in four adult Americans are currently offered an online personal health record, by a health plan or physician's office, most have not taken up the offer.

Google, Microsoft and WebMD all say they will not show advertising alongside a person's health records. But visitors to WebMD, Google Health and Microsoft's site, HealthVault, see ads for drugs for diseases like osteoporosis or acid reflux as they seek information on an array of ailments.

Technology experts say identities of viewers and their health interests are often captured at the moment they click on online ads for a drug. That provides the advertiser with a prospective customer to pursue online or by mail.

"Personal health records linked to advertising, even indirectly, put them in the hands of marketers and profilers," said Robert Gellman, an independent privacy consultant in Washington.

Microsoft and WebMD acknowledge that the privacy rules in the stimulus law apply to them. **Google says the law's prohibitions do not apply to it**, except for its duty to report any breaches of medical privacy. "Google is bound by the privacy policy that people agree to when they sign up," said Christine Chen, a Google spokeswoman.

...

Full article: http://www.nytimes.com/2009/08/09/business/09privacy.html

---

From Google's web site:

*"**Is Google Health covered by HIPAA?** Unlike a doctor or health plan, **Google Health is not regulated by the Health Insurance Portability and Accountability Act (HIPAA)**, a federal law that establishes data confidentiality standards for patient health information. This is because Google does not store data on behalf of health care providers. Instead, our primary relationship is with you, the user. Under HIPAA, you have a right to obtain a copy of your medical records. If you choose to use Google Health, we'll help you store and manage your medical records online."*

http://www.google.com/intl/en-US/health/about/

Hi, my name is Sherri Davidoff. I'm a computer forensic investigator and a network security professional. One of my jobs is to assess the security of my clients' networks. Over the past decade, I have had the opportunity to see inside the computer networks of many different types of organizations, including health care institutions, government agencies, financial instutions, retailers, telecommunications companies, and more. I've had the opportunity to see first hand the types of information these organizations collect, and how well they manage-- or don't manage-- their security. From a personal perspective, what I have seen is frightening. I am here today to tell you a little bit about it.

When you go to the store, and you buy a box of cold medicine, or a book, or ammunition, and you pay with a card, that information is recorded. The credit card issuer tracks the location, date, time and type of each purchase. The store itself may track very granular information about your purchases, such as the names of the movies you buy or the caliber, type and quantity of ammunition you purchased.

Your purchase histories, including what you purchased, where and when, is then sold to marketers, insurance companies, the federal government, pretty much anyone who is willing to pay for it.

This has become a huge industry.

When you walk around on the street, your cell phone tracks you everywhere you go. The FCC required that all cell phones have highly granular GPS tracking capabilities, for the purposes of emergency 911 calls. However, software writers and mobile carriers use this to keep detailed location histories of YOU which they use for their own profit. Software writers who create apps on your phone can record your location as you travel, and sell records of your location history to whomever they want! When you visit someone's house, when you go to the bar, you can be tracked and your location records can be sold to marketers, insurance companies, the federal government, anybody.

Your medical prescription information is not private the way you think it is. Prescription information has been bought and sold for decades. In recent years, the federal government has been passing stronger laws regarding medical data privacy. Unfortunately, the budgets of health care organizations are often very stretched, and they often do not have the resources to comply, or to properly secure sensitive medical information. I have seen this countless times with my own two eyes. In Montana, medical information is not included as "personal information" under our state data breach notification law, so under state law, data holders are not required to notify you if your medical information is stolen.

Now that health information is becoming electronic, companies like Google are offering medical record storage and management services. These companies are NOT health care providers and they are NOT required to abide by HIPAA, which limits how medical information can be distributed.

There are many companies that track your web browsing habits online. When you visit a web site or type information into your computer, your web browsing history is tracked and sold. The words you type into searches are tracked and sold. This can include health information, financial information, your interests and habits. If you think it's anonymous, guess again. Have you ever typed your own name or address into your computer? Have you ever bought anything online with your credit card? Have you ever entered your email address or a blog username linked to your real name? There are companies which specialize in figuring out your real name and matching that to your web browsing history, which is frequently and invisibly tracked by third parties.

There are also companies that collect your web browsing history, and tie that into your purchase histories (from credit cards or stores), motor vehicle records, medical information, and much more. These detailed personal "dossiers" about YOU are sold to advertisers, financial institutions, governments and more for profit. Companies can use them for price disrimination, marketing different products and prices to you based on the information they have. Banks could deny you loans based on your web surfing history. This information is extremely valuable, and extremely dangerous.

You would think that companies carefully secure this extremely personal information, but most of the time, they don't. If your credit card number gets stolen, and nobody finds out about it, is there any cost to the merchant? If your health information is stolen, and the company that was keeping it never tells anyone, will they suffer any loss themselves? There's little incentive for the companies trading this personal information to invest a lot of resources in keeping your most private data secure. Instead, they just use it, sell it, and try to minimize their own costs. As a result, the more your personal information is bought and sold, the higher your risk for identity theft.

I am proud to be a Montanan. I am proud to live in a state where citizens have a Constitutional right to privacy, and are willing to stand up for it. Over the past decade, technology has moved so quickly that the law hasn't been able to keep up.

As a result, Montana citizens are being constantly exploited. Our movements are being tracked. Our purchases are being recorded and sold. Our activities are being watched. Most of the time, this happens invisibly, without our knowledge and without our consent.

I believe that this is directly opposite of what our constitutional framers intended, and what most Montana citizens would want. We don't want to be bought and sold. We value our freedom here, and our privacy.

It is time for us to catch up with technology, to conduct a study, and to examine the ways that we can protect Montana citizens, while still balancing the needs of our state and local governments, and our business community.